Module 8   Mandatory Access Control and Labels   Exam

1)   Which TCSEC classes require MAC?

    a)   C1 and C2.
    b)   B1, B2 and B3.
    c)   A1.
    d)   a) and b).
    e)   b) and c).
    f)   None of the above.

2)   A sensitivity label represents the sensitivity of information through:

    a)   a hierarchical level only.
    b)   a hierarchical category set only.
    c)   a non-hierarchical level and a hierarchical category set.
    d)   a hierarchical level and a non-hierarchical category set.

3)   Integrity labels:

    a)   address the denial-of-service problem.
    b)   in the Biba model are the dual of secrecy (sensitivity) labels in theBell-LaPadula model.
    c)   are identical to secrecy labels.
    d)   are required to implement multilevel security.
    e)   a) and d).

4)   Covert channels are:

    a)   a TCSEC concern at C2.
    b)   a designated means to transfer information.
    c)   dominated by the subject's ability to access an object.
    d)   a means by which information is signaled in a manner that violates the system's security policy.
    e)   None of the above.

5)   Human-readable sensitivity markings for human-readable output are not required until what class?

    a)   C2.
    b)   B1.
    c)   B2.
    d)   B3.
    e)   A1.

6)   The TCSEC "Label Integrity" requirement specifies that (selectas many as are applicable):

    a)   only the TCB may set subject and object sensitivity label values.
    b)   integrity labels must exist.
    c)   labels exported from the TCB must be unambiguously associated with an object.
    d)   administrators must be trusted to assign labels.
    e)   covert channel bandwidths must be limited.

7)   A covert channel is a concern not because a cleared user can use thechannel, but because a Trojan horse can use the channel.

    a)   TRUE.
    b)   FALSE.

8)   The two types of covert channels are:

    a)   timing channels and communication channels.
    b)   timing channels and storage channels.
    c)   storage channels and communication channels.
    d)   random channels and communication channels.
    e)   None of the above.

9)   A trusted backup program that is allowed to violate DAC but not allowedto violate MAC would have to be running at _____ in order to be able to backup all files on the system.

    a)   system-low.
    b)   system-high.

Questions 10 and 11 refer to a system having the levels from highest to lowest of T, S, C, U and the two categories A (Apples) and O (Oranges).

10)   A security clearance of S with category A dominates:

    a)   T with no category.
    b)   S with category O.
    c)   C with category A.
    d)   U with category A and O.
    e)   b) and c).
    f)   c) and d).
    g)   None of the above.

11)   A security clearance of C with category A and O is dominated by:

    a)   T with category O and A.
    b)   S with category O.
    c)   C with no category.
    d)   U with category A and O.
    e)   a) and b).
    f)   b) and c).
    g)   c) and d).

The following information applies to questions 12 through 14:

Subject	Current Clearance
Moe	SECRET (NATO, NUCLEAR, CRYPTO)
Curly	TOP SECRET (NATO, NUCLEAR)
Larry	SECRET (NATO, CRYPTO)
Shep	TOP SECRET ()

Object	Current Classification
Cream Pie	CONFIDENTIAL (NATO, CRYPTO)
Pointy Object	SECRET (NUCLEAR)
Shaved Poodle	TOP SECRET (NATO, NUCLEAR)

The MAC implementation allows read-down and write-up.

12) Who can read the Cream Pie?

a) Moe.
b) Curly.
c) Larry.
d) b) and c).
e) a) and c).
f) None of the above.

13) Who can write the Pointy Object:

a) Moe.
b) Larry.
c) Shep.
d) a) and c).
e) b) and c).
f) None of the above.

14) Who can execute the Shaved Poodle?

a) Moe.
b) Larry.
c) Shep.
d) a) and b).
e) b) and c).
f) None of the above.